

# IP Control

## User Guide



[www.minicom.com](http://www.minicom.com)

International HQ

Jerusalem, Israel

Tel: + 972 2 535 9666  
[minicom@minicom.com](mailto:minicom@minicom.com)

North American HQ

Linden, NJ, USA

Tel: + 1 908 486 2100  
[info.usa@minicom.com](mailto:info.usa@minicom.com)

European HQ

Dübendorf, Switzerland

Tel: + 41 44 823 8000  
[info.europe@minicom.com](mailto:info.europe@minicom.com)

Technical support - [support@minicom.com](mailto:support@minicom.com)

# Table of Contents

<b>1. Welcome.....</b>	<b>3</b>
<b>2. Introduction .....</b>	<b>4</b>
<b>3. Key features .....</b>	<b>4</b>
<b>4. System components.....</b>	<b>4</b>
<b>5. The IP Control unit .....</b>	<b>5</b>
<b>6. Pre-installation guidelines.....</b>	<b>5</b>
6.1 Avoiding general rack mounting problems .....	6
<b>7. Rack mounting the IP Control .....</b>	<b>6</b>
<b>8. Terminology .....</b>	<b>7</b>
<b>9. Client computer operating system.....</b>	<b>7</b>
<b>10. Connecting the system.....</b>	<b>7</b>
<b>11. Initial settings - Default IP address .....</b>	<b>9</b>
11.1 Static IP addresses for a number of units .....	10
<b>12. Logging into the Web interface .....</b>	<b>11</b>
12.1 SSL Certificate notes .....	12
<b>13. Network &gt; Configuration .....</b>	<b>12</b>
13.1 LAN 1 .....	12
13.2 KVM.net.....	13
<b>14. Network &gt; SNMP settings.....</b>	<b>13</b>
<b>15. Administration &gt; User Settings .....</b>	<b>14</b>
15.1 Adding a user .....	15
15.2 Editing a user .....	15
15.3 Deleting a user .....	15
15.4 Blocking a user.....	15
<b>16. Administration &gt; Switch Configuration.....</b>	<b>16</b>
<b>17. Administration &gt; Serial Settings .....</b>	<b>17</b>
17.1 Show .....	17
17.2 Assign to RPS .....	17
<b>18. Security &gt; Settings .....</b>	<b>18</b>
<b>19. Security &gt; SSL Certificate .....</b>	<b>18</b>
<b>20. Maintenance &gt; Firmware Upgrade.....</b>	<b>19</b>
<b>21. Restore Factory Settings.....</b>	<b>20</b>
<b>22. Saving changes and logging out.....</b>	<b>20</b>
<b>23. Starting a remote session .....</b>	<b>21</b>
23.1 Taking over a busy remote session.....	22
23.2 Moving or hiding the Toolbar.....	22
23.3 Switching to a different server/device .....	23
23.4 Changing the performance settings .....	23
23.5 Adjusting the Video settings .....	24
23.5.1 Refresh.....	24
23.5.2 Manual Video Adjust.....	24
23.5.3 Auto Video Adjust .....	25

23.6 Power cycle .....	26
23.7 Keyboard key sequences .....	26
23.8 Synchronizing mouse pointers .....	27
23.8.1 Aligning the mice pointers .....	28
23.8.2 Calibrating mice pointers .....	28
23.8.3 Manual mice synchronization .....	28
23.9 Minicom logo menu features .....	30
23.10 Full screen mode.....	31
23.11 Disconnecting the remote session .....	31
<b>24. Troubleshooting - Safe mode.....</b>	<b>31</b>
24.1 Entering Safe mode .....	31
24.2 Restoring factory defaults .....	33
24.3 Restoring the device firmware .....	34
<b>25. Technical specifications.....</b>	<b>35</b>
<b>26. Video resolution and refresh rates.....</b>	<b>36</b>
<b>27. Safety.....</b>	<b>36</b>
<b>28. User guide feedback.....</b>	<b>36</b>
<b>29. WEEE compliance .....</b>	<b>36</b>

© 2008 Copyright Minicom Advanced Systems. All rights reserved.

# 1. Welcome

Thank you for buying the IP Control system. This system is produced by Minicom Advanced Systems Limited.

This document provides installation and operation instructions for Minicom's IP Control. It is intended for system administrators and network managers, and assumes that readers have a general understanding of networks, hardware and software.

## Technical precautions

This equipment generates radio frequency energy and if not installed in accordance with the manufacturer's instructions, may cause radio frequency interference.

This equipment complies with Part 15, Subpart J of the FCC rules for a Class A computing device. This equipment also complies with the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications. These above rules are designed to provide reasonable protection against such interference when operating the equipment in a commercial environment. If operation of this equipment in a residential area causes radio frequency interference, the user, and not Minicom Advanced Systems Limited, will be responsible.

Changes or modifications made to this equipment not expressly approved by Minicom Advanced Systems Limited could void the user's authority to operate the equipment.

Minicom Advanced Systems Limited assumes no responsibility for any errors that appear in this document. Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Minicom Advanced Systems Limited.

## Trademarks

All trademarks and registered trademarks are the property of their respective owners.

## 2. Introduction

The IP Control extends your KVM (keyboard, video, mouse) from any computer or server over TCP/IP via LAN, WAN or Internet connection. Now you can control, monitor and manage your servers from wherever you are, inside or outside the organization. The IP Control is a cost-effective hardware solution, for secure remote KVM access & control of a computer/server from the BIOS level - independent of the OS. It is designed to connect to a single computer or to a KVM switch to control multiple servers, over TCP/IP communication.

## 3. Key features

**BIOS level control** to any server's brand and model, regardless of the server condition and network connectivity, covering the entire spectrum of crash scenarios.

**Compatible** with all major operating systems. Supports many hardware and software configurations for the remote client and the target server computers, as well as the KVM switch in use.

**Web-based Control** - Browser based control of a target server, from any location via secured standard IP connection.

**Multi-user view mode** - Allows simultaneous users to view remote sessions. Remote control can be intuitively handed between users with appropriate permissions.

## 4. System components

The IP Control system consists of:

- 1 IP Control (p/n 1SU70017)
- 1 KVM cable (p/n 5CB00565)
- 1 RS232 cable (p/n 5CB00566)
- 1 Universal power adapter (p/n 5PSB0005)
- Rack mount set (p/n 5AC00297)

The RS232 cable connects the IP Control to Serial manageable devices such as Power Management units, routers, etc.

## 5. The IP Control unit

Figure 1 illustrates the front panel of the IP Control.

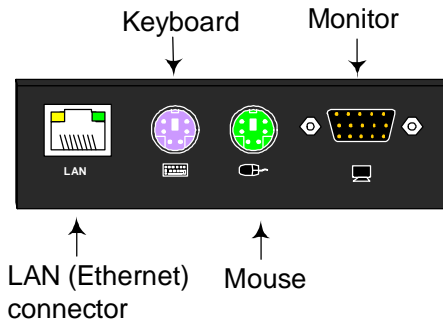


Figure 1 IP Control ports – side 1

For (optional) local access to the connected computer you connect a keyboard, monitor and mouse to the above KVM ports. Connect the IP Control to a 10/100 Mbit Ethernet using the LAN port.

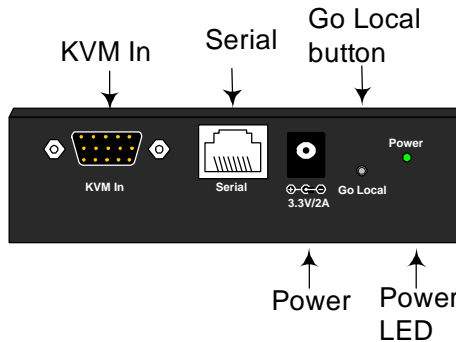


Figure 2 IP Control ports – side 2

Connect a computer or KVM switch to the KVM In port using the 1 to 3 CPU cable. You press the **Go Local** button to disconnect the remote session and access the computer locally.

Connect an RS232 device to the Serial port using the RS232 cable.

## 6. Pre-installation guidelines

Place cables away from fluorescent lights, air conditioners, and machines that are likely to generate electrical noise.

## 6.1 Avoiding general rack mounting problems

### Elevated operating ambient temperature

The operating ambient temperature of the rack environment may be greater than the room ambient when installing into a closed or multi-unit rack assembly. So install the equipment in an environment compatible with the maximum rated ambient temperature.

### Reduced airflow

Install the equipment in a rack in such a way that the amount of airflow required for safe operation is not compromised.

### Mechanical loading

Mount the equipment in the rack in such a way that a hazardous condition is not achieved due to uneven mechanical loading.

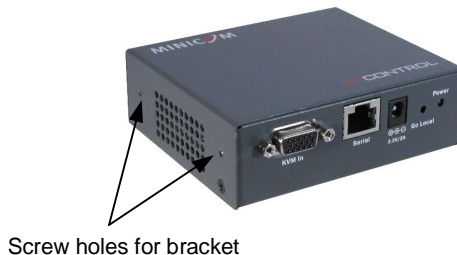
### Circuit overloading

When connecting the equipment to the supply circuit, consider the effect that overloading of circuits might have on over-current protection and supply wiring.

Reliable earthing of rack-mounted equipment should be maintained. Give attention to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

## 7. Rack mounting the IP Control

The IP Control comes with screw holes on the side for easy rack mounting, see figure below.



**Figure 3 Screw holes for rack mounting**

Use the L-shaped brackets and screws provided to mount the IP Control on a server rack or under a table top as illustrated below. The length of the screws used for connecting the brackets to the IP Control unit must not exceed 5 mm.



Screw L-shaped brackets to 1 or both sides of the unit

**Figure 4 Connecting the L-shaped bracket**



**Figure 5 Connected to a rack**



**Figure 6 Connected to a table top**

## 8. Terminology

Below are some terms and their meanings used in this guide.

Term	Meaning
<b>Target server</b>	The computers/servers that are accessed remotely via the IP Control.
<b>Client computer</b>	The PC running a remote IP Control session
<b>Remote Session</b>	The process of accessing and controlling Target Servers connected to IP Control from a User workstation

## 9. Client computer operating system

Windows 2000 or higher, with Internet Explorer 6.0 or later version. 128 bit encryption support is required.

## 10. Connecting the system

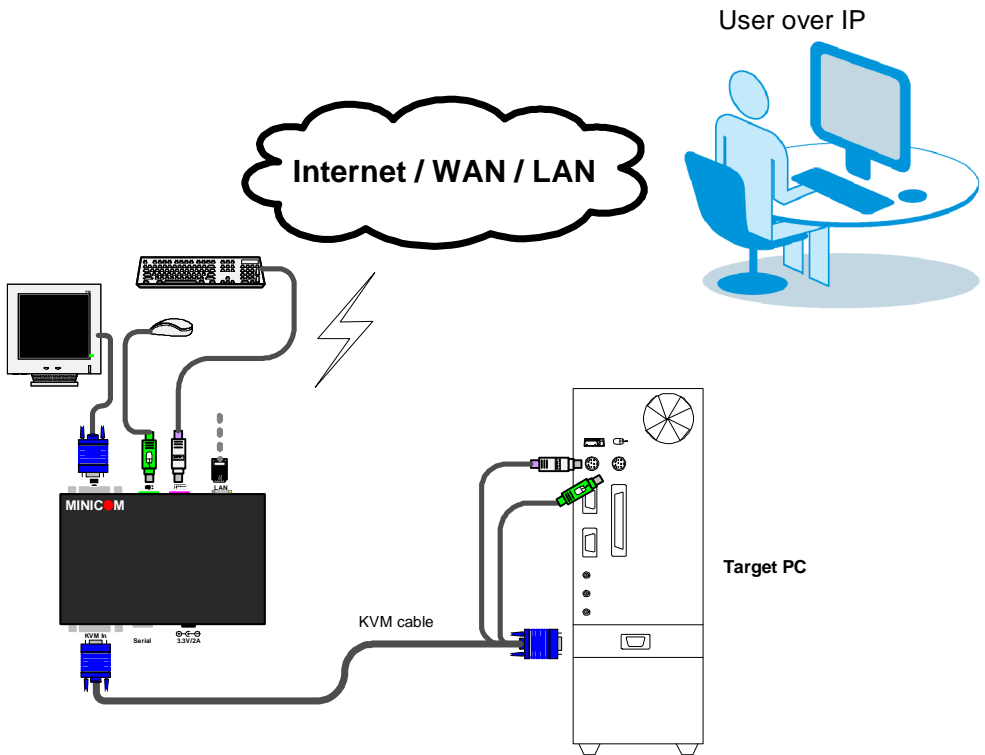
Connect the Target Server / KVM switch to the IP Control as follows:

1. Connect the single connector of the KVM cable to the KVM In port of the IP Control.



2. Connect the other end of the KVM cable to the KVM ports of the Target Server / KVM switch.
3. Connect a Network cable to the IP Control LAN port and to an Ethernet port on your Network switch.
4. Connect the power adapter.

Figure 7 and Figure 8 illustrate the connections to a computer and KVM switch respectively, with the optional KVM console.



**Figure 7 IP Control connections to a computer**

User over IP

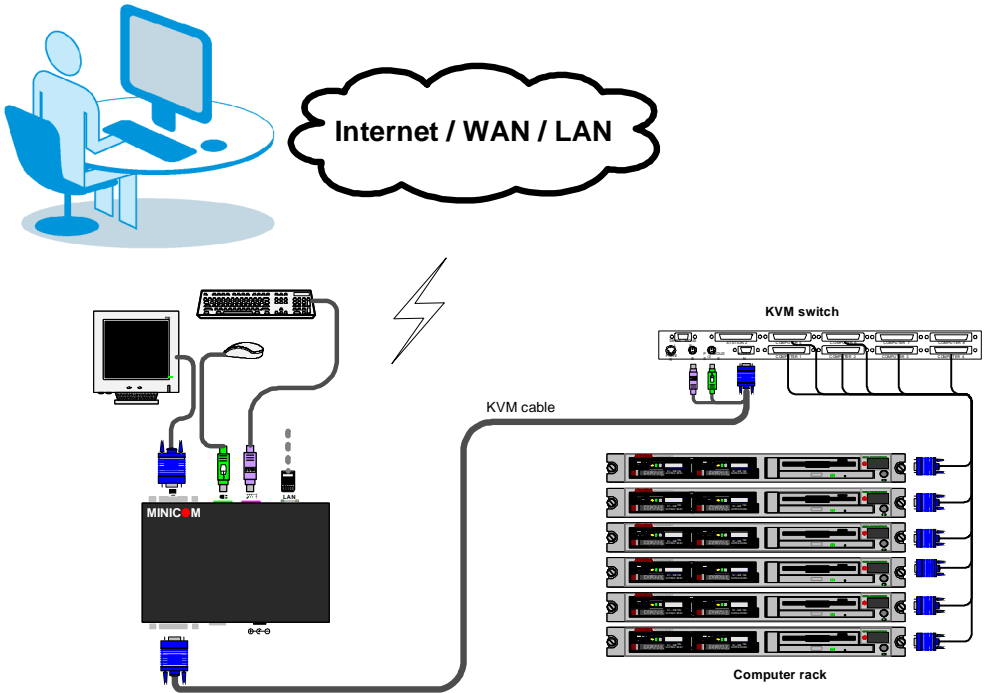


Figure 8 IP Control connections to a KVM switch

## 11. Initial settings - Default IP address

The following sections provide instructions for setting the IP address for the IP Control unit.

See Figure 9 for an overview of the boot-up process.

By default, IP Control boots with an automatically assigned IP address from a DHCP (Dynamic Host Configuration Protocol) server on the network. The DHCP server provides a valid IP address, gateway address and subnet mask.

To identify the IP address, the IP Control MAC address appears on the underside of the IP Control box. The device number (D.N.) can also be found there.

If no DHCP server is found on the network, IP Control boots with the static IP address: 192.168.0.155.

**Note!** If a DHCP server later becomes available, the unit picks up the IP settings from DHCP server. To keep the static IP address, disable DHCP – explained in section 13.1 on page 12.

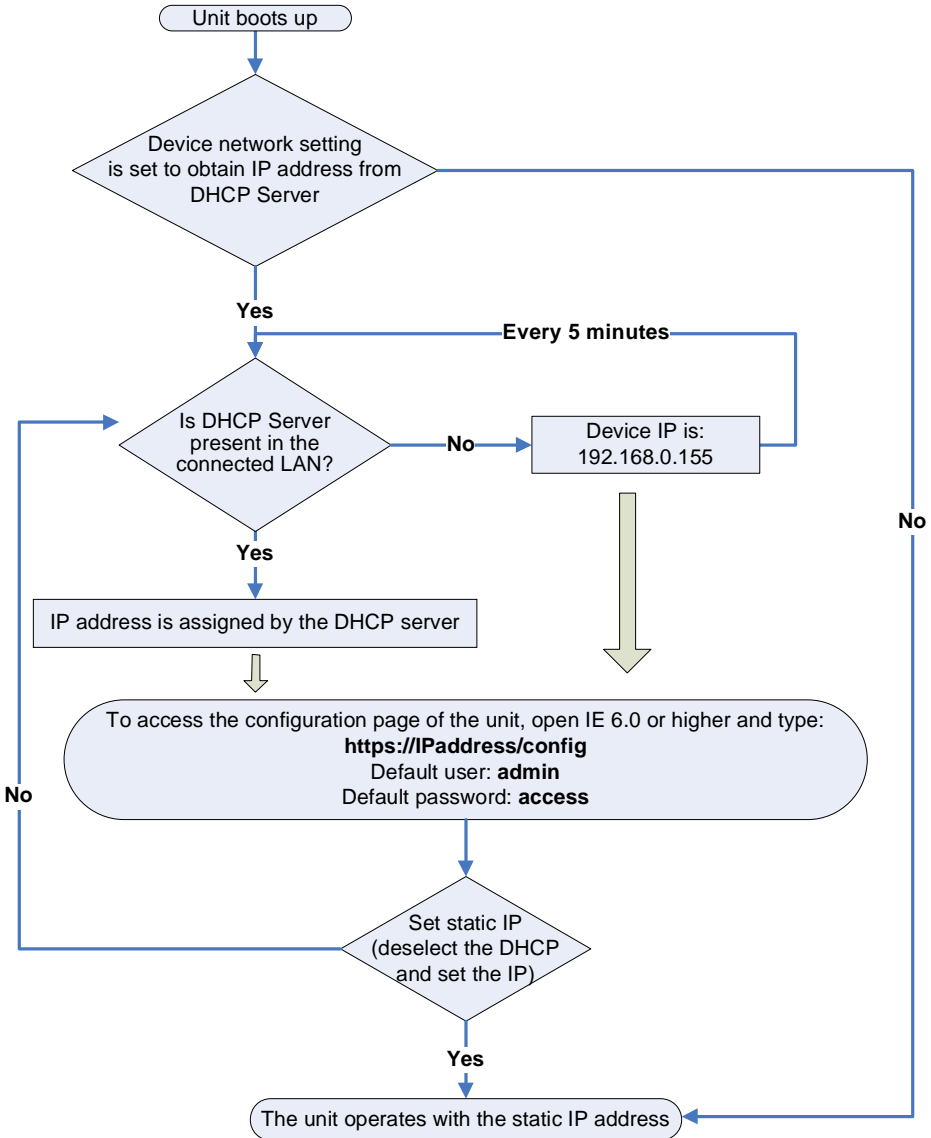


Figure 9 Boot-up process

## 11.1 Static IP addresses for a number of units

Where you want to connect more than 1 IP Control to the same network and there is no DHCP server, or you want to use static IP addresses, do the following:

Connect the IP Control units one at a time and change the static IP address of each unit before connecting the next unit.

## 12. Logging into the Web interface

Complete the initial setup via the Web configuration interface:

1. Open your Web browser (Internet Explorer version 6.0 or higher).
2. Type the IP Control system IP address - `https://IP address/config` - and press **Enter**. The login page appears, see Figure 10.

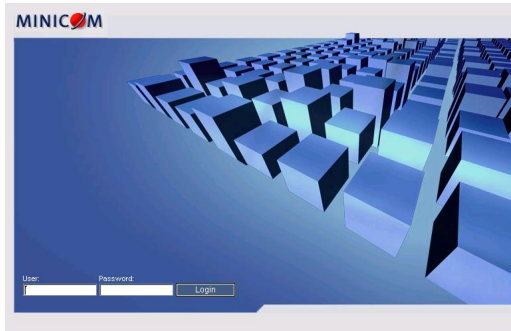


Figure 10 Login page

3. Type the default Administrator user name **admin** and password **access** (both lower case).
4. Press **Enter**. The Web interface opens at the Network Configuration page. See Figure 11.
5. Bookmark the page for easy reference.

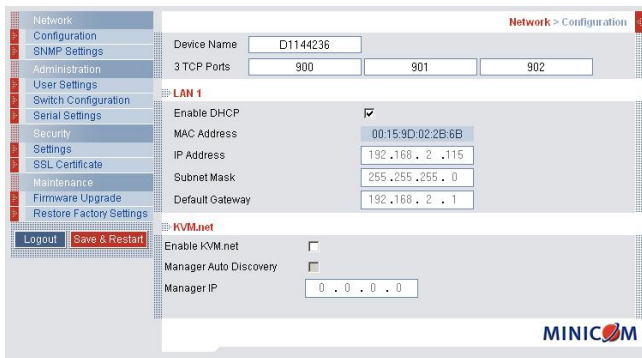


Figure 11 Configuration page

## 12.1 SSL Certificate notes

When first connecting to IP Control's configuration page, 2 browser security warnings appear. Click **Yes** to proceed.

The first warning disappears upon first IP Control client installation, when Minicom's root certificate is installed.

## 13. Network > Configuration

Consult your Network Administrator for the network settings.

**Device name** - Type a name for the IP Control. Default device name consists of the letter 'D' followed by the 6-digit device number (D.N.) found on the silver label on the underside of the IP Control box. If the DHCP server is published in the DNS server, you may connect to the IP Control using the device name, as follows:

`https://DeviceName`

**TCP Ports** - Choose any 3 TCP ports from port #800 to 65535. (When managed by KVM.net<sup>®</sup> II, the port numbers can be changed from KVM.net interface if needed).

### Note

Firewall or router security access list must enable inbound communication through the selected TCP ports for the IP Control's IP address.

For Client computer access from a secured LAN, the selected ports should be open for outbound communication.

### 13.1 LAN 1

Under LAN 1 in Figure 11, is the following:

**Enable DHCP** – When a DHCP server is active on the same network to which IP Control is connected, DHCP provides automatic IP assignment.

When DHCP is disabled – (Recommended) – You can assign a fixed IP address to the IP Control.

Consult your Network Administrator regarding the use of the DHCP.

**Note!** Where you have access to the server – your configured (or default) IP Control device name will appear on the DHCP server's interface, making it easy to locate.

When DHCP is disabled, enter the **IP Address**, **Subnet Mask**, and **Default Gateway** for **LAN 1**, as given by your Network Administrator.

## 13.2 KVM.net

KVM.net is a centralized IP based system for secure control of servers and network devices, power and user administration in the data center environment. KVM.net combines Out-Of-Band, KVM via IP access with modern IT standards and requirements. It is the most comprehensive remote server maintenance solution available in the market today.

**Enable KVM.net** - Check this option to allow IP Control to be remotely managed by Minicom's KVM.net system.

**Manager Auto Discovery** – when checked, KVM.net automatically detects the IP Control, if it resides on the same network segment.

**Manager IP** – If IP Control resides on a different segment, type the static IP address of the KVM.net Manager. (We advise typing the static IP address of the KVM.net Manager even if the IP Control resides on the same network segment as the KVM.net Manager).

## 14. Network > SNMP settings

From the menu click SNMP settings. The following appears.

**SNMP:**



Enable traps: ☐

Community:

SNMP Manager IP:

**Figure 12 SNMP settings**

From this page you can activate or deactivate SNMP logging.

**Enable traps** - Check to enable SNMP traps of IP Control events and operation.

**Community** – type the SNMP community.

**SNMP Manager IP** - Enter the SNMP Server IP address.

## 15. Administration > User Settings

From the menu click **User Settings**, Figure 13 appears.

User	Permission	Status
1. admin	Administrator	

**Figure 13 User Settings**

On this page an Administrator creates and edits users.

There are 3 levels of user access:

- Administrator
- User
- View only

### Administrator

An Administrator has unrestricted access to all windows and settings and can “take over” any active session (explained in section 23.1 on page 22). An Administrator can change the name and password of all users.

### User

A User can access/control Target Servers, but cannot use the following:

- Advanced mouse settings
- Power cycle


A User has no access to the Web configuration interface.

### View only

View only can view the screen of any Target Server without keyboard and mouse control. A “view only” indicator appears on the viewer’s local mouse pointer.


## 15.1 Adding a user

To add a user:

1. Click  and type a name and a password. The password must be at least 6 characters – letters or numbers, and must not include the user name, even if other characters are added.



**Note!** The following “special” characters: &, <, >, ” cannot be used for either the user name or password.

Depending on the security level chosen the user name and password parameters are different. See section 18 on page 18.

2. Select the permission type from the **Permission** drop down menu.
3. Click , the user appears in the list of users.



## 15.2 Editing a user

To edit a user:

1. Select the user from the list.
2. Click . You can now change all the parameters – user name, permission and password.
3. Click , the changes are saved.

## 15.3 Deleting a user

To delete a user:

1. Select the user from the list.
2. Click .
3. Click , the changes are saved.

## 15.4 Blocking a user

An alternative to deleting a user is blocking a user. This means that the user’s name and password is stored, but the user is unable to access the system. Check **Block** to block a user. Uncheck **Block** to allow the user access.



## 16. Administration > Switch Configuration

When a KVM switch is connected to the IP Control system, you must configure the switch parameters.

To do so:

1. From the menu click **Switch Configuration**. The KVM Switch Configuration window appears, see Figure 14.

Server Name	
1	Server1
2	UNUSED
3	UNUSED
4	UNUSED
5	UNUSED
6	UNUSED
7	UNUSED
8	UNUSED
9	UNUSED
10	UNUSED
11	UNUSED
12	UNUSED
13	UNUSED
14	UNUSED
15	UNUSED
16	UNUSED

Figure 14 Switch Configuration

2. Choose the manufacturer and model of the connected KVM switch. The number of possible connected servers appears in the **Server Name** section.
3. Change the name of the connected servers by highlighting the server and typing a new name. Click **Apply** to save changes.

**Note!** Server names left as **UNUSED** cannot be accessed.

### Install switch definition file

Where the KVM switch type is not listed in the manufacturer/model drop-down lists, you can find the correct Switch Definition file in the Support section of our website - <http://www.minicom.com/phandlj.htm>.

1. Load the file onto the Client computer.
2. Locate and install the KVM switch definition file. The switch definition file is replaced.

## 17. Administration > Serial Settings

Where you have a Serial device connected to the system you must configure the RS232 settings.

To do so:

From the menu click **Serial Settings**, the **Serial Settings** appear, see Figure 15.

Administration > Serial Settings

Serial Port

Device Name:  CharSet:

Baud Rate:  Data Bits:

Parity:  Stop Bits:

Show: ☒ Assign to RPS: ☐

**Figure 15 Serial Settings**

Type a device name and choose the correct device parameters.

**Note!** Where you have a Minicom Serial Remote Power Switch connected, see below **Assign to RPS**.

### 17.1 Show

Tick **Show** to make the Serial device appear in the list of servers/devices that can be accessed.

### 17.2 Assign to RPS

Where a Minicom Serial Remote Power Switch (RPS) is connected to the Serial port, tick this box. All other parameters are then grayed out. See the RPS Installation Guide for further information on installing and operating the RPS.

## 18. Security > Settings

Configure the security features, such as Account Blocking, Password Policy and Idle Timeout, as explained below.

From the **Security** section click **Settings**, the **Security Settings** appear, see Figure 16.

Security > Settings

**Account Blocking**

Block after  attempts within H  M

Block account for H  M  ☐ forever

**Password Policy**

☐ High security password policy

**Idle Timeout**

Disconnect after  min. of inactivity

Figure 16 Security Settings

The security Settings elements:

**Account Blocking** – decide on the number of attempts to login with a wrong username or password after which there is a time lock or a total block.

**Password Policy** – You have the option of a standard or high security level of password. The table below shows the parameters of the 2 options.

Standard security policy	High security policy
6 characters or more	8 characters or more must include at least 1 digit and 1 upper case letter and 1 "special" character as follows !@#%&^*()_-=[]';?/{}
Must not include the user name	Must not include the user name

Check the box to enable the high security password policy. Unchecked, the standard security policy applies.

**Idle Timeout** – Select the Timeout inactivity period after which the user is disconnected from the system. Choose **No Timeout** to disable Timeout.

## 19. Security > SSL Certificate

You can install an SSL certificate.

To do so:

From the menu, select **SSL Certificate**, the install SSL Certificate page appears, see Figure 17.

**Figure 17 Install SSL Certificate page**

**Certificate File** - Browse to locate the **cer** file.

**Private File** - Browse to locate the **private key** file in Microsoft pvk format.

**Key Password** - Type the “private key” password.

Click **Save & Restart**.

## 20. Maintenance > Firmware Upgrade

Upgrade the IP Control firmware to take advantage of new features. Download the firmware from Minicom’s website at:

<http://www.minicom.com/phandlh.htm>.

Save the firmware file on the Client computer.

From the menu select **Firmware Upgrade**. The Firmware Upgrade appears see Figure 18.

**Figure 18 Firmware Upgrade**

1. Locate and upload the firmware file.
2. Verify the current and uploaded version of the firmware.
3. Click **Start Upgrade**. The upgrade starts. On completion, click **Reboot**. The unit reboots. After about 30 seconds the Login page appears.

**Note!**

Depending on the type of firmware upgrade, the following settings may be erased: User settings, KVM switch settings, mouse and video adjustments and RS232 settings. For more information refer to the firmware release notes.

The network settings remain intact.

## 21. Restore Factory Settings

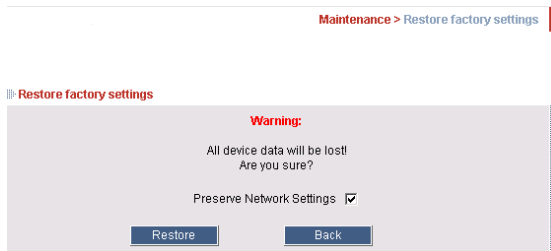
You can restore the IP Control unit to the factory settings. This restores the original IP Control parameters, resetting all the information added by the administrators, including: Network settings\*, Servers, Switches, Users, Passwords etc.

\* You have the option to preserve Network settings – explained below.

**Warning! Once reset the data cannot be retrieved.**

To restore factory settings:

1. From the menu select **Restore Factory Settings**. Restore Factory Settings appears see Figure 19.



**Figure 19 Restore factory settings**

2. Check the box if you want to preserve Network settings.
3. Click **Restore**.

## 22. Saving changes and logging out

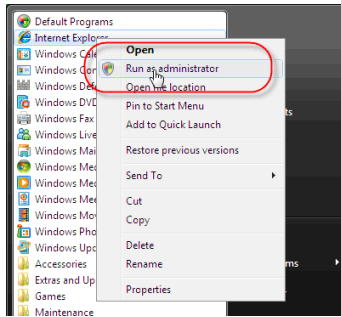
Click **Save & Restart** to save any configuration changes and restart the IP Control system.

To exit the Configuration menu and close the session, click **Logout**.

Only one Administrator can log into the Configuration area at a time. An idle timeout of 30 minutes terminates the session.

## 23. Starting a remote session

**Windows Vista Note!** To login to the web interface with Windows Vista, run Internet Explorer as Administrator. To do this, right-click the Internet Explorer icon on the Taskbar and select Run as administrator. See Figure 20.



**Figure 20 Select Run as administrator**

At a Client computer open Internet Explorer (6.0 and above) and type the IP Control's IP address. <https://IP address>. The Login page appears. Type your username and password and press Enter. By default, the user name is: **admin** and the password is **access**, (both lower case).

On first connection install the Minicom certificate and ActiveX control. You must login as an Administrator to your computer to install the ActiveX control. Once the ActiveX control is installed, all types of users can login.

The screen of the Target Server connected directly to IP Control, or the currently selected server on the KVM switch with IP Control toolbar appears see Figure 21.

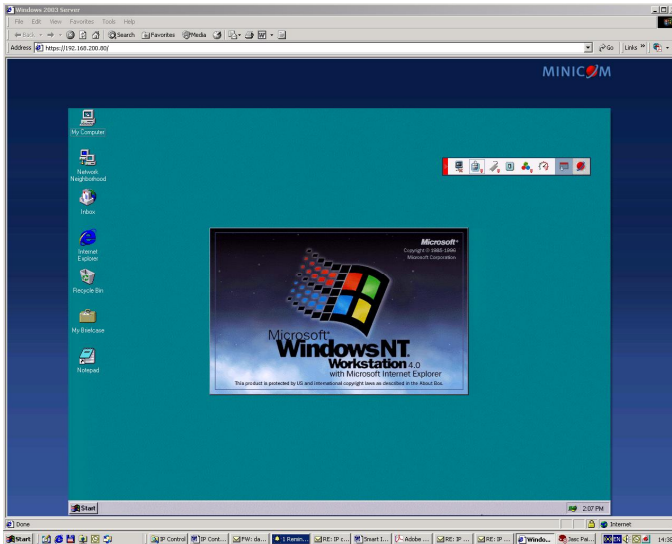


Figure 21 Remote session window

## 23.1 Taking over a busy remote session

When connecting to a busy Target Server an Administrator has the option to take over the Target Server. A User only has this option when the current session is run by another User, but not by an Administrator. The following message appears




Figure 22 Busy remote session options

Choose to Take Over or View Only or Cancel.

## 23.2 Moving or hiding the Toolbar

The Toolbar can be dragged and dropped to anywhere on the screen, by clicking

and dragging the logo .

To hide the Toolbar, either:


Double-click the IP Control System tray Icon .

Or press **F9**.

To display the Toolbar repeat the above actions. See also page 30.



To minimize the Toolbar:



Click the arrow . Click again to maximize the Toolbar.

### 23.3 Switching to a different server/device

To connect to a different server/device:

1. From the Toolbar, click , or right-click . A list of connected servers/devices appears.
2. Click the desired server or Serial device. The screen of the server or the Serial device window appears.

### 23.4 Changing the performance settings

In a LAN environment, it is best to leave the bandwidth setting on High. For VPN and internet environments you may want to alter the settings to increase responsiveness.

You can alter the bandwidth settings from the Toolbar.

To alter the settings:



From the Toolbar, click . The Settings.. box appears, see Figure 23.

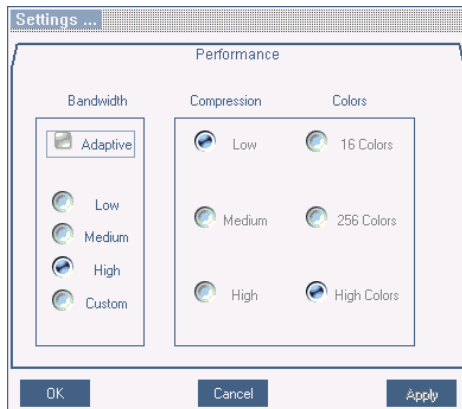


Figure 23 Settings.. box

#### Bandwidth

Choose from the following options

**Adaptive** – automatically adapts to the best compression and colors according to the network conditions.

**Low** - Select Low for high compression and 16 colors.



**Medium** - Select medium for medium compression and 256 colors. Medium is recommended when using a standard internet connection.

**High** - For optimal performance when working on a LAN, select High. This gives a low compression and high colors (16bit).

**Custom** – You can choose your own compression and color levels.

Click **OK**. The chosen setting take effect and the screen of the last accessed Target Server appears.

## 23.5 Adjusting the Video settings

To change the video settings:

From the Toolbar, click . You have the following options:

- Refresh
- Manual Video Adjust
- Auto Video Adjust

Each option is explained below.

### 23.5.1 Refresh

Select Refresh to refresh the Video image. Refresh may be needed when changing the display attributes of a Target Server.

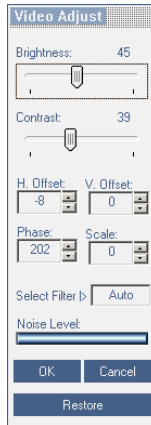
### 23.5.2 Manual Video Adjust

Use the manual video adjustment for fine-tuning the Target Server video settings after auto adjustment or for adapting to a noisy environment or a non-standard VGA signal or when in full-screen DOS/CLI mode.

To adjust the video manually:

Click Manual Video Adjust. The manual controls appear, see Figure 24. Also a red frame appears around the screen. This represents the screen area according to the Server's screen resolution. Perform the adjustments inside and relative to this frame.

After adjusting the video manually, you can always revert to Auto settings by clicking Auto Video Adjust – explained in section 23.5.3 below.



**Figure 24 Manual Video Adjustments controls**

**Brightness / Contrast** - use the scales to adjust the brightness and contrast of the displayed image. Move the sliders to change the displayed image. Click in the area of the sliders for fine-tuning.

For the following controls choose the appropriate measurement.

**Horizontal Offset** - defines the starting position of each line on the displayed image.

**Vertical Offset** - defines the vertical starting position of the displayed image.

**Phase** - defines the point at which each pixel is sampled.

**Scale** – defines the scale resolution of the session image.

Adjust Phase and Scale to reduce noise level to a minimum.

**Select Filter** - defines the filter of the input video from the server. A higher filter reduces the noise level but makes the image heavier.

**Noise Level** - represents the Video "noise" when a static screen is displayed.

### 23.5.3 Auto Video Adjust

To adjust the video automatically:

Click **Auto Video Adjust**. The process takes a few seconds. If the process runs for more than 3 times, there is an abnormal noise level. Check the video cable and verify that no dynamic video application is running on the Target Server's desktop.

Perform the procedure where necessary for each Target Server or new screen resolution.

## 23.6 Power cycle

Where a Minicom Remote Power switch is connected to the Serial port of the IP Control, you can power manage the Target servers as follows:

From the Toolbar, click . The Power menu appears, see below.

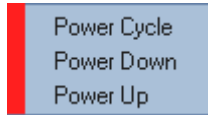



Figure 25 Power menu

To send a power cycle command or to power down or up the currently accessed Target server, select the appropriate option.

**Note!** Only the currently accessed Target server is affected, so to power manage other Target servers you must access each one individually.

## 23.7 Keyboard key sequences

Click . A list of defined keyboard sequences appears. When clicked, these transmit directly to the Target Server, and will not affect the Client computer.

For example, select **Ctrl-Alt-Del** to send this three key sequence to the Target Server to initiate its Shutdown/Login process.

To add a keyboard sequence:

Click **Add/Remove**. The Special Key Manager box appears see Figure 26.

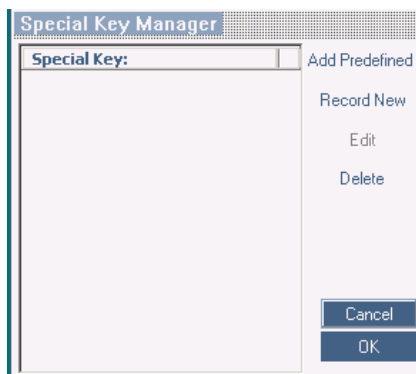


Figure 26 Special Key Manager box

To add a predefined sequence:

1. Click Add Predefined. A list of sequences appears.

2. Select the desired sequence and click OK. The sequence appears in the Special Key Manager box.
3. Click OK. The sequence appears in the Keyboard Key sequence list.

To record a key sequence:

1. From the Special Key Manager box press **Record New**. The Add Special Key box appears see Figure 19.

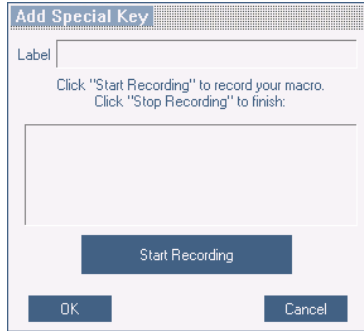


Figure 27 Add Special Key box

2. Give the key sequence a name in the Label box.
3. Click **Start Recording**.
4. Press the desired keys. The keys appear in the area provided.
5. Click **Stop Recording**.
6. Click **OK**.

To edit a key sequence:

1. From the Special Key Manager box select the desired key.
2. Click **Edit**.
3. Click **Start Recording**
4. Press the desired keys. The keys appear in the area provided.
5. Click **Stop Recording**.
6. Click **OK**.

## 23.8 Synchronizing mouse pointers

When working at the Client computer, two mouse pointers appear: The Client computer's is on top of the Target Server's. The mouse pointers should be synchronized. The following explains what to do if they are not synchronized.


### Warning

Before synchronizing mouse pointers adjust the video of the Target Server, (explained above) otherwise mouse synchronization may not work..

#### 23.8.1 Aligning the mice pointers

When accessing the Target Server, the mice may appear at a distance to each other.


To align the mouse pointers:

From the Toolbar click  / **Align** or press **Ctrl+M** simultaneously. The mice align.

#### 23.8.2 Calibrating mice pointers

A Target Server may have a different mouse pointer speed to the Client computer. Calibrating automatically discovers the mouse speed of the Target Server and aligns the two pointers.

To perform the calibration when the Target Server Operating system is, Windows NT4, 2000 or 98:

From the Toolbar click  / **Calibrate**. IP Control saves this alignment so calibration is only needed once per Target Server.

If the Video Noise Level is above zero, calibration may not work. Go to Video Adjustment and try to eliminate the noise by pressing Auto video adjust and/or adjusting the bars in Manual video adjust, then perform the mouse calibration.

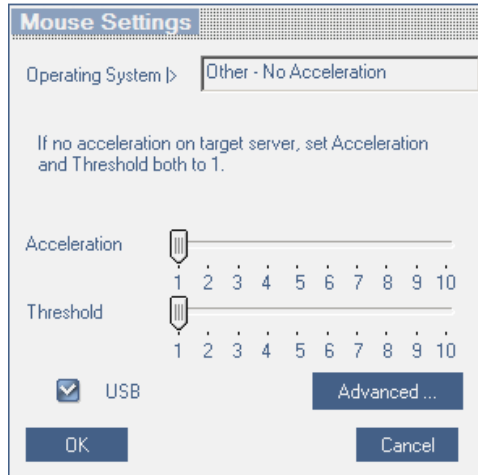
**Note!** If the mouse settings on the Target Server were ever changed, you must synchronize mouse pointers manually, as explained below.

#### 23.8.3 Manual mice synchronization

If the mouse settings on the Target Server were ever changed, or when the Operating system on the Target Server is, Windows XP / 2003 Server / Vista /2008 Server, Linux, Novell, SCO UNIX or SUN Solaris you must synchronize the mouse pointers manually.

To manually synchronize mouse pointers:

1. From the Toolbar click  / **Manual Settings**. The **Mouse Settings** box appears see Figure 28.




**Figure 28 Mouse Settings box**

2. Select the Target Server's Operating System and click OK. Instructions and sliders appear.
3. Follow the instructions and set any relevant sliders to the same values as set in the Target Server's Mouse Properties window.

## **2 examples!**

For Windows XP, go to the Mouse settings on the Target Server and uncheck Enhance pointer precision.

For Windows NT4. If Mouse Properties were ever changed for the Target Server – even if they have been returned to their original state - uncheck default -  Default.

Click **OK**. The mouse pointers should be synchronized.

### **23.8.3.1 USB**

The USB option in Mouse Settings box is available for ROC/RICC and X-RICC USB, USB to PS/2 adapter, Phantom Specter USB and for unsupported operating systems and SUN Solaris. Use this option if you are sure of the custom acceleration algorithm you are using, or have been informed so by customer support.

### **23.8.3.2 Advanced – Mouse Emulation**

In the Advanced Mouse settings, you can set the type of mouse that you would like IP Control to emulate. We recommend not changing the advanced settings unless there is erratic mouse behavior (the mouse is making random clicks and jumping arbitrarily around the screen).


Click  the Mouse Emulation box appears see Figure 29.



Figure 29 Mouse Emulation box

Select the mouse connected to the Local Console port on the IP Control, e.g. if the local mouse is a non-Microsoft 2 button mouse, select **Standard Mouse** and uncheck **Microsoft Mouse**.

**Max Rate** - this defines the maximum mouse report rate. For Sun Solaris the default value is 20 in order to support older Sun versions.

## 23.9 Minicom logo menu features



Right click the Minicom logo, a menu appears. From this menu you can access the connected devices. You also have the following features:

**Disconnect** – You can disconnect the session by clicking Disconnect.

**About** - Click About to verify the Client, Firmware, KME (Keyboard/Mouse Emulation firmware) and Switch file versions installed on your IP Control.

**Local Settings** – Click Local settings, the Client Configuration box appears, see Figure 30

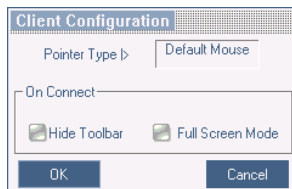


Figure 30 Client Configuration box

**Pointer type** – From the Drop-down list you can change the Client computer mouse pointer to appear as a dot or to not appear at all.

**Hide Toolbar** – Check this option to hide the Toolbar from the next reconnection onwards. To toggle the Toolbar on and off, press **F9**. See above page 22.

**Full Screen Mode** - Check this option to make the remote session screen appear in full screen mode from the next reconnection onwards. To toggle the full screen mode on and off, press **F11**. (See section below).

## 23.10 Full screen mode

Work on the Target Server as if you are working on a local computer, with full screen mode.

To work in full screen mode:


1. Ensure that the Client computer has the same screen resolution as the Target Server.
2. Press **F11**. The Internet Explorer window disappears, leaving the Internet Explorer menu bar at the top.
3. Right click the Internet Explorer menu bar and check Auto-Hide. The Internet Explorer menu bar disappears. You are in full screen mode.

To exit full screen mode:

Press **F11**. Or place the mouse at the top of the window to display the Internet Explorer toolbar and click the Restore button.

**Note!** Full screen mode can also be activated from the Toolbar menu, see page 30. (Click Minicom logo in the System tray).

## 23.11 Disconnecting the remote session

To disconnect the session, on the Toolbar, click . The Login box appears. You can re-login or close the browser window.

## 24. Troubleshooting - Safe mode

From the Safe mode you can:

**Restore factory defaults** - When you cannot access the system e.g. you have forgotten the Username or Password, restore factory defaults from the Safe mode. (Section 21 on page 20 explained how to restore factory settings from the web interface).

**Restore the device firmware** – If during a firmware update there is a power failure and you can no longer access the system you can restore the device firmware from the Safe mode.

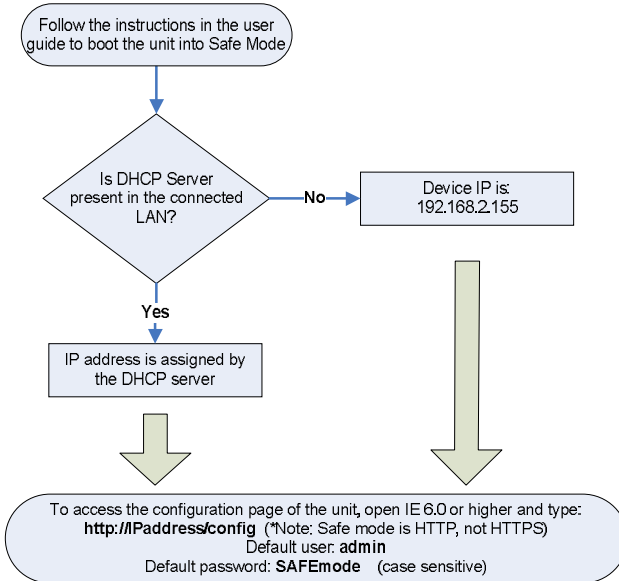
### 24.1 Entering Safe mode

To enter Safe mode:

1. While powering up the IP Control, press and hold down the Go Local button for 3-4 seconds. The device boots up in Safe mode.

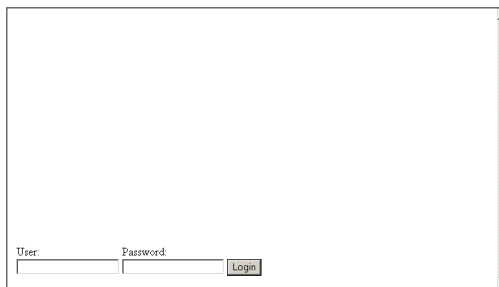


2. Wait until the unit finishes booting (1-2 minutes).
3. You need to know the IP address of the IP Control. The IP address depends on whether there is a DHCP server on the network. If there is, the DHCP server assigns an IP address to the IP Control. If there is no DHCP server, the unit boots with the static IP address 192.168.2.155. See Figure 31 for an overview of this procedure.



**Figure 31 Safe mode procedure**

Open Internet Explorer and type the following into the Address box: `http://IP address/config`. (Do not start the address with **https**). The Login page appears, see Figure 32.



**Figure 32 Login page**

4. Type username: **admin** , password: **SAFEmode**. (Case sensitive). (This username and password works only in Safe mode). A menu appears, see Figure 33.

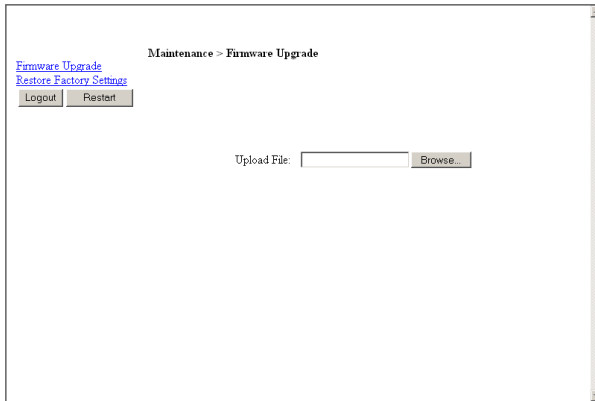


Figure 33 Safe mode menu

## 24.2 Restoring factory defaults

To restore factory defaults:

1. From the menu choose **Restore Factory Settings**. A warning appears see Figure 34.

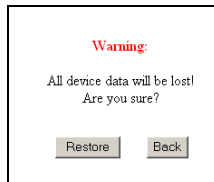


Figure 34 Warning

2. Click **Restore**. A further warning appears, see below.



Figure 35 Warning

3. Click OK, the factory defaults are restored. When the process finishes Figure 36 appears.



Figure 36 Reboot

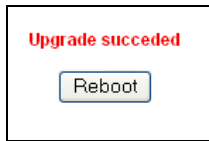
4. Click **Reboot** to restart the unit.

## 24.3 Restoring the device firmware

Contact Minicom Technical Support [support@minicom.com](mailto:support@minicom.com), to receive the Upgrade firmware required to restore the device firmware. Save the Upgrade firmware on the hard disk of a computer connected to the network.

To restore the device firmware:

1. From the Safe mode menu choose Firmware Upgrade.
2. Locate the Upgrade firmware and click Install, then click Start Upgrade. The firmware upgrades. When the process finishes Figure 37 appears.



**Figure 37 Reboot**

3. Click **Reboot** to restart the unit.

## 25. Technical specifications

<b>Operating systems</b>	<b>Target Server</b> DOS, Windows, Novell, Linux, SUN Solaris for PC <b>Client Computer</b> Windows 2000 or higher with IE 6.0 or higher and ActiveX
<b>Resolution</b>	<b>Target Server</b> Up to 1600 x 1200 @ 85Hz <b>Client Computer</b> Recommended - resolution should be higher than on Target Server
<b>Video and mouse synchronization</b>	Both auto and manual modes
<b>Security</b>	128-bit SSL encryption
<b>Connections</b>	<b>Ethernet</b> – RJ45 – 10/100 Mbit/sec autosensing <b>Serial</b> – RJ45 <b>Local KVM connection</b> – Screen HDD15, Keyboard./Mouse – MiniDIN6 <b>Computer / switch connection</b> –HDD15, KVM cable 1.8m. Monitor HDD15, Keyboard./Mouse – MiniDIN6
<b>Weight</b>	0.2kg / 0.45lb
<b>Dimensions (H x D x W)</b>	3 x 10 x 8 cm / 1.1 x 3.9 x 3.1in
<b>Power adapter</b>	3.3VDC, 2 A.
<b>Operating temperature</b>	0°C to 40°C / 32° to 104°F
<b>Storage temperature</b>	-40°C to 70°C / -40°F to 158°F
<b>Humidity</b>	80% non condensing relative humidity

## 26. Video resolution and refresh rates

Hz →	56	60	65	66	70	72	73	75	76	85	86
640x480		x		x	x	x		x		x	
720x400					x					x	
800x600	x	x				x		x		x	x
1024x768		x			x	x	x	x	x	x	
1152x864								x			
1152x900				x					x		
1280x720		x									
1280x768		x						x			
1280x960		x								x	
1280x1024		x				x		x	x	x	
1600x1200		x	X		x			x		x	

## 27. Safety

The device must only be opened by an authorized Minicom technician. Disconnect device from the power source and all cables from the device before service operation!

## 28. User guide feedback

Your feedback is very important to help us improve our documentation. Please email any comments to: [ug.comments@minicom.com](mailto:ug.comments@minicom.com)

Please include the following information: Guide name, part number and version number (as appears on the front cover).

## 29. WEEE compliance

WEEE Information for Minicom Customers and Recyclers

Under the Waste Electrical and Electronic Equipment (WEEE) Directive and implementing regulations, when customers buy new electrical and electronic equipment from Minicom they are entitled to:

- Send old equipment for recycling on a one-for-one, like-for-like basis (this varies depending on the country)
- Send the new equipment back for recycling when this ultimately becomes waste

Instructions to both customers and recyclers/treatment facilities wishing to obtain disassembly information are provided in our website [www.minicom.com](http://www.minicom.com).

## Regional Offices

### Germany

Kiel

Tel: + 49 431 668 7933

[info.germany@minicom.com](mailto:info.germany@minicom.com)

### France

Vincennes

Tel: + 33 1 49 57 00 00

[info.france@minicom.com](mailto:info.france@minicom.com)

### Italy

Rome

Tel: + 39 06 8209 7902

[info.italy@minicom.com](mailto:info.italy@minicom.com)

### England

Tel: + 44 121 288 0608

[info.uk@minicom.com](mailto:info.uk@minicom.com)

### China

Tel: +86 21 6445 3181

[info.china@minicom.com](mailto:info.china@minicom.com)

### Asia Pacific / S. Korea

Tel: +972 2 535 9618

[info.ap@minicom.com](mailto:info.ap@minicom.com)

[www.minicom.com](http://www.minicom.com)



